JMTPR
Journal of Management Theory and Practices Research

Journal of **M**anagement **T**heory and **P**ractices **R**esearch
Cilt/Volume :2 | Sayı/Issue: 2 | Aralık/December 2021

SİBER GÜVENLİK BAĞLAMINDA YENİ TEHDİT ALGILAMALARININ TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

Ozan Zeki KİRAZ[1]

Makale İlk Gönderim Tarihi / Recieved (First): 05.10.2021 **Makale Kabul Tarihi / Accepted:** 04.11.2021

Atıf/©: Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. Journal of Management Theory and Practices Research, 2(2), 69-88

Özet

Bu çalışmanın amacı, Türkiye'de siber güvenlik politikalarının güvenlikleştirme ve risk algısı üzerindeki etkisini araştırmaktır. Hem devletler hem özel sektör, izleme ve gözetleme araçlarının kullanımını arttırmaktadır. Elektronik iletişimin izlenmesi, elektronik kimlik tespiti, e-imza, e-devlet, kamusal alanda olan kamera sistemleri gibi teknolojiler gündelik hayatımızda olağan karşılanmaktadır. İnternet yoluyla gerçekleşen insan hakları ihlalleri internetin gelişimi ile birlikte artmıştır. Bu ihlallerin toplum üzerindeki etkisi olmaktadır. Siber zorbalık, internette çocuk istismarı, yetkisiz erişim, özel hayatın gizliliğini ihlal, banka bilgilerinin ele geçirilmesi ve diğer siber suçlar internet yoluyla gerçekleşen insan hakları ihlalleridir. Siber suçların caydırıcı olabilmesi için ciddi hukuki düzenlemelere ihtiyaç duyulmaktadır. İnternet yoluyla işlenen İnsan hakları ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir. Bilinçli kullanılırsa teknolojinin faydaları olabilir. Özellikle Çocuklarımızın ve gençlerin internet bağımlılığı konusunda bilinçlenmesi gerekmektedir. Herkes siber suçla karşılaşabileceğinden herkes siber güvenlik önlemi almalıdır. Çalışmadan çıkarılabilecek en temel sonuç siber güvenlik herkes tarafından önemli hale gelmiştir ve bu güvenliğin tesis edilmesinde herkese görevler düşmektedir.

Anahtar Kelimeler: İnternet Bağımlılığı, Siber Güvenlik, Siber Hukuk, Siber Zorbalık.

THE IMPACTS OF NEW THREAT PERCEPTİONS ON TURKEY'S SECURITY POLICIES IN THE CONTEXT OF CYBER SECURITY

Citation/©: Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. Journal of Management Theory and Practices Research, 2(2), 69-88

Abstract

The aim of this study is to investigate the impact of securitization and risk perception of cyber security policy in Turkey. Both the governments and the private sector increase the use of monitoring and surveillance tools. Technologies such as electronic communication monitoring, electronic identification, e-signature, e-government, and camera systems in public space are considered as normal in our daily lives. Human rights violations through the internet have increased with the development of the internet. These violations have a great impact on society. Cyberbullying, child abuse on the internet, unauthorized access, violation of privacy, seizure of bank information, and other cybercrime are human rights violations through the internet. Serious legal regulations are needed for cybercrime to be a deterrent. In order to prevent human rights violations committed through the internet, both public and private sectors have important duties. Technology can have benefits if used consciously. Especially children and young people need to be conscious about internet addiction. Everyone should take cyber security precautions, as everyone can come across cybercrime. The main conclusion that can be drawn from the study is, Cyber security has become important for everyone and everyone has a role to play in establishing this security.

Keywords: İnternet Addiction, Cyber Bullying, Cyber Law, Cyber Security.

1 Batman Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı, ozanzekikiraz@gmail.com, ORCID 0000-0002-6584-2810

1. GİRİŞ

İnternetin ve teknolojinin gelişmesiyle etkileşim boyutu da değişmiş ve dönüşmüştür. İletişim kanalları tarih boyunca gelişerek insanlığı da geliştirmiştir. Siber Uzay da milyarlarca kullanıcı olup anlık olarak etkileşim halindedir ve bu durum ulus devletler için kendi halklarının üzerinde kontrolünü kaybetme endişesiyle karşı karşıya bıraktırmıştır. Karar alıcılar, otoriteler, yöneticiler ve tüm bireyler siber uzayda küresel doğanın parçasıdırlar ve birbirlerine network ağları ile bağlıdırlar. Bu sebeple disiplinler arası çalışma ile birlikte küresel çapta bir bakış açısıyla konunun çalışılması gerekmektedir.

Çalışmanın temel konusu, siber güvenliğin sağlanması açısından yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkilerini incelemektir. Bu konunun seçilmesinin sebebi ise siber güvenliğin gelişen ve merak edilen dünyasına bir katkı sunmasıdır. Özellikle özele indirgenecek olunursa Türkiye'nin güvenlik politikalarında siber güvenlik ne derece önem arz ediyor, gereken önlemler alınıyor mu ve tehditlere karşı hangi kurumlar çalışmakta olduğu araştırılmıştır.

Siber güvenlik konusu uluslararası güvenlik çalışmaları içinde önemli bir yerde olup insan hakları hukuku açısından da önemi giderek artmıştır. Siber suçların, insan haklarına olan müdahalesini azaltmak için siber güvenliğe özel önem verilmesi gerekmektedir. Bu güvenliği sağlamanın da o kadar kolay olmadığı ve devletlere, sivil toplum kuruluşlarına, uluslararası kuruluşlara veya şirketlere bir takım görevler düştüğü anlaşılmıştır.

Teknolojinin gelişimi genel anlamda insanlığa olumlu katkılar sunmuş olup anlık iletişim, doğrudan ve kesintisiz iletişim, maliyetlerin düşürülmesi gibi daha bir çok katkı sunmuştur. Basit olarak örnek verilecek olursa sosyal medya ve uygulamalar ile anlık, doğrudan ve maliyetsiz iletişim sağlanmıştır.

Teknolojik gelişmeler kadar bu gelişmelerin sonucu ortaya çıkan ürünlerin doğru kullanımı da insanların sağlığı ve gelişimi için önemlidir. Eğer telefon ve bilgisayar bağımlılığı olursa psikolojik sorunlardan sağlık sorunlarına kadar zararlar olabilecektir. Bir başka örnek olarak yalan veya yanlış bilgilerin yayılarak provokasyon ve tahrik edici bilgiler sonucu insanlarda korku ve panik yaratacak haberler sıklıkla yapılabilmektedir. Bu bilgilerin çürütülmesi veya doğru bilgilerin yerini alması zaman alabilmektedir.

Sosyal medyanın kullanımın yaygınlaşması ile birlikte kamuoyu oluşumu ve bir düşünce üzerinde birliktelik hızlanmıştır. Sivil toplum kuruluşlarının çabasıyla oluşturulabilecek kamuoyu faaliyeti twitter sosyal platformunda kolaylıkla sağlanabilmektedir. Özellikle bu kanaat ve düşünceler sonucu ortaya çıkan sonuçlar üzerine "twitter adaleti" söylemi ortaya çıkmıştır.

Teknolojinin gelişimi kamuoyu oluşumu ve oluşturma biçimlerini etkilemiştir. Günümüzde kamuoyu kavramı çok sık kullanılmakta olup "Kamu" terimi ile toplulukları veya grupları ifade ederken, "oy" terimi ile bir kanaati ve yönelimi ifade eder. Kamuoyu kavramı genellikle bir sorun veya mesele karşısında bu meseleyle ilgili olan gruplarının kanaatlerini veya görüşlerini anlatmaktadır (Kapani, 2008: 160-161).

Sosyal Medyada da belli bir fikir, düşünce veya tutumun kamuoyu oluşturulmaya çalışılarak yaygınlaştırılmaya çalışıldığı çok sık görülebilmektedir. Bunun en iyi örneği twitter platformunda kullanıcıların konu başlığı olarak bilinen "hashtag" oluşturulması ve bu konu üzerinde yaygın düşünce, eğilim ve kanaat oluşturacak şekilde paylaşım yapılması çok sık karşılaşılmaktadır. Bu sosyal medyanın gücünü göstermesinin yanı sıra kitleleri ve toplumu yönlendirmede anlık ve güçlü bir etkisi olduğunu göstermektedir. Bu tıpkı bir lobicilik faaliyeti gibi baskı grubu olmuştur. "Sosyal medya adaleti" veya

"Twitter Adalet Bakanlığı" gibi adlandırmalar veya söylemler sıklıkla telaffuz edilir olmuştur.

Ulus devletlerin dış politikalarında artık uluslararası propaganda önemli hale gelmiştir. Özellikle Birinci Dünya Savaşı sonrası sık olarak kullanılan propaganda, iletişim teknolojisinin ilerlemesi ile birlikte yaygınlaşmaya başlamıştır. Propaganda, bir grubun düşünce veya siyasetini etkilemek için tasarlanmış olan ve yaratılan faaliyetlerdir diye tanımlanabilir. Genellikle devletlerin diplomatik faaliyetlerin uzantısı olup devletlerin etkinliğini dış politikada arttırmalarında araç olarak kullanılmaktadır (Arıboğan, Ayman, Dedeoğlu; 2005: 676-677).

Siyasi liderler başta olmak üzere siyasi aktörler sosyal medyanın gücü ile dinleyici hedeflerine kolay şekilde ulaşmaya ve bundan maksimum olarak faydalanmaya çalışmaktadırlar. Siyasi kurum ve liderleri; kampanyalarını, pazarlayacakları argümanlarını, kamu diplomasisi ve halkla ilişkilerini en süratli ve ekonomik (maliyetsiz) olarak sosyal medya araçlarının imkânları ile sağlayabilmektedirler (Cihangir, 2020: 194).

Sosyal medyada paylaşılan haberlerin ve bilgilerin kitleleri harekete geçirme gücü hafife alınmamalıdır. Sosyal medyada kamuoyu oluşturmak ve olmamış ya da yaşanmamış konuların yayılması sıklıkla karşılaşılan bir durumdur. Bu nedenle sosyal medya mecralarında algı oluşturmak basit hale gelmiştir. Bir siber saldırı ile siyasi olsun olmasın kişilerin ya da kurumların imajlarını psikolojik olarak zedelemek mümkündür. Karalama propagandaları yapılarak takipçilerinin veya taraftarlarının gözünden düşürebileceği gibi gizli bilgi belgelere erişilerek ifşa veya şantaj yapılma suretleriyle gündemde sansasyonel olay yapılabilmektedir.

Bir siber saldırının sadece siyasi ya da sadece ekonomik kazanç elde etme amacı ile yapılmaz. Saldırı yapıldığında sonuçları siyasi, ekonomik ve imaj bozulması gibi birçok sonucu olabilmektedir. Siber saldırılar hangi amaç veya hedef için yapılırsa yapılsın etkileri ve sonuçları büyük olabilmektedir. Tedbirlerin sağlıklı olup olmadığı acil durum veya siber saldırılarla karşı karşıya kalındığında anlaşılacaktır. Zararın boyutunu en aza indirmenin yolu bu alana yatırım yapılmasını zorunlu hale getirmektedir. Sonuçların ağır olmaması daha önce alınmış bir önlem ve tedbirin olup olmamasına bağlı olarak değişmekte olup güvenliğin sağlanması için sadece devletlerin değil birçok kurum, kuruluş ve bireylerinde katkı yapması gerekmektedir.

Siber güvenlik günümüz dünyasında aşama aşama artarak küresel bir güvenlik sorunu haline gelmiştir. Bu sebeple bu konu seçilip araştırma yapılmış olup teknik bilimlerde olduğu gibi sosyal bilimlerde artan önemine katkı sunması amaçlanmıştır. Bir başka amaçlanan unsur bireylerin de siber güvenliklerini sağlamasının önemidir. Bilgisayar virüsleri sadece bilgisayara ve işletim sistemine zarar vermekle kalmıyor insanların psikolojilerini de etkilemek başta üzere birçok zarar verebilmektedir. Siber güvenlik konusunda en zayıf halka birey olup dikkatsiz ve özensiz kullanımı ile birçok zarara sebebiyet verebilmektedir. Bu çalışma bireylerinde farkındalık kazanması açısından dikkat çekmeye çalışmıştır.

2. KAVRAMSAL ÇERÇEVE

Dünya genelinde siber suçlar olarak bilinen suçlar dikkat çekici şekilde artmış olup siber güvenliğin önemi artmıştır. Siber güvenlik sadece kurum ve kuruluşların değil bireyler için de önem kazanmıştır.

2.1. Siber Güvenlik Kavramı

Günümüze gelene kadar siber güvenlik kavramı ile genel olarak teknik sorunları ve aksaklıkları gidermek olarak anlaşılmıştır. Ancak siber güvenlik kavramı sadece teknik sorunları değil insan ya da kullanıcı hatası sonucu oluşan problemlerin ortadan kaldırılmasını da içermektedir. Hem teknik hem

sosyal boyutu ile değerlenme yapılması gerektiği için bu alan özellikle disiplinler arası bir işbirliği yapılmasını zorunlu hale getirmiştir. Siber güvenliğin üç ana hedefi bulunmaktadır: Bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumaktır. Bilgiye kim ulaşacak, kim değiştirebilecek ve son olarak bilgiye kim istediği zaman erişebilecek sorularının cevabı aranmaktadır (Akyeşilmen, 2018: 13-14).

Siber güvenlik (cyber security), genel hatları ile siber alanda olan bilginin

1. mahremiyetinin (confidentiality),
2. bütünlüğünün (integrity),
3. ulaşılabilirliğinin (availability) korunması olarak ifade edilebilmektedir (Güvenlik Terimleri Sözlüğü, 2017: 621).

Siber güvenlik, bir bilişim sistemi kullanıp sağlıklı bir iletişim kurulmasını ve bu iletişimin içeriğini de kapsayacak şekilde güvenliğini kapsamaktadır. Daha detaylı olarak incelenirse iletişimin hem sağlıklı ve güvenli olmasını hem de iletişimin içeriğinin (ses, mesaj vs.) ne ile iletişim kuruluyorsa ilgisiz kişilere karşı (üçüncü kişilere karşı) güvenliğini de içermektedir. Gerçekten de siber güvenliğin sağlanması için verilerin bütünlüğü, gizliliği, saklanması, paylaşılacak ise ulaşacağı kanallar sistemin güvenliği için önemlidir.

Siber güvenlik sektöründe yerli ve milli cihazların geliştirilmesi, siber güvenliğin güvenilirliği anlamında büyük önem taşımaktadır. Yurt dışından alınmış olan ürünlerin, cihazların ve/veya programların istismar edilme olasılığı yüksektir. Alınan sistemin güvenilirliği tartışmalı olmanın yanı sıra ülkenin mevcut ekonomik durumuna yük getirmektedir. Her ülke kendi yerel kaynaklarını kullanarak yerli ürünler, cihazlar ve programlar geliştirirse kendi güvenliğine katkı sağlamış olacaktır. Tabi bu yüzde yüz tam anlamıyla bir güvenliği ifade etmemektedir. Her sistemin bir açığının olabildiği akılda bulundurulması gerekmektedir. Siber saldırılar çok sık olarak karşılaşılmaktadır. Bunlar karşısında önlem almayan veya dijitalleşen ve gelişen dünyada siber alana yatırım yapmayan devletler kaybeden taraf olacaklardır.

Siber güvenlik günümüzde tek bir ürün tarafından veya tek bir kurum aracılığıyla sağlanması imkânsız gibi görünmektedir. Bu nedenle Savunma Sanayi Bakanlığı, Emniyet ve Türk Silahlı Kuvvetlerin ilgili Siber Başkanlıkları veya birimleri, Bilgi Teknolojileri Kurumu ve ilgili birimler koordineli şekilde çalışmaları zorunlu hale gelmiştir. Yapay zekâ, robot teknolojileri, güvenlik sistemleri ve büyük data (veri) teknolojilerinde bilgi paylaşımı ve ortak plan oluşturma ihtiyacı geçen zamandan daha çok artmıştır.

Havacılık sektöründe gelişen ve çıkış yaşayan İHA ve/veya SİHA araçları başarılı sonuçlar almışlardır. Aynı şekilde uydu teknolojileri, siber güvenlik, yazılım ve simülasyon alanlarında da yerli teknolojiler geliştirilmesine ihtiyaç vardır. Bunun için yeterli düzeye sahip insan kaynağının da yetiştirilmesi ve mümkünse ilkokul veya ortaokul çağından itibaren eğitim verilmesi gerekmektedir. Özel sektör girişimcilerinin doğmasına da izin verilmeli, böylelikle dünyadaki rekabet ortamında faaliyet göstermeleri olanaklı hale getirilmelidir.

Türk firmalarının da öncelikle Asya, Afrika, Balkanlar ve Orta Doğuda yarışabilir hale gelmesi sağlanmalı, daha sonra da sektörde büyük devletlerde bulunan firmalarla rekabet edebilir düzeye gelmesi gerekmektedir. Aksi durumda Türkiye'nin müdahale edici ve etkin rolünün azalacağı bir pozisyona düşmesi kaçınılmazdır.

2.2. Siber Uzayın Tanımlanması

İnternet sadece dijital bir dünyayı ifade etse bile siber uzay insanı kapsamaktadır. Dolayısıyla siber uzay, sistemi ve teknolojisiyle insanın yapmış olduğu bir üründür (Akyeşilmen, 2018: 53).

Siber uzay; kullanıcılardan, yazılımlardan, küresel ağlardan oluşan ve elektronik veri kaynaklı sanal bir dünyayı ifade etmektedir. Şeffaf bir alan olsa dahi sırları ve gizemini içerisinde barındırmaktadır. Bilinmezlikler ve muğlaklıklar bu alanda çok fazladır. Bu nedenle tehlikeli ve riskli bir alan olduğundan dolayı yönetilmesi ve kontrolü zordur (Akyeşilmen, 2018: 58).

Siber Uzay oluşumunu, fiziksel alandan sanal alana yaklaştıran katmanlardan biri olan kodlar katmanı ile gerçekleşmektedir. Fiziksel katman unsurları olarak bilinen ana kartlar, işlemciler, RAM'ler kodlar ile kullanılır duruma gelmektedir. "Doğru-Yanlış" ve ya "1-0" olacak şekilde programlama dilleri aracılığıyla işlemcinin nasıl çalışacağı belirlenir (Bıçakçı, 2014: 108).

Tıpkı fiziksel uzay gibi siber uzayın da derinliği ve boyutu bilinememektedir. Diğer taraftan siber uzay aynı fiziksel uzay gibi sürekli genişlemekte ve büyümektedir. Buna bir örnek verecek olursak her saniye, dakika, gün ve zaman insanlar internet âlemine yapmış olduğu veya çoğalttığı resim, video, yazı, ses veya her türlü bilgi yükleyerek siber uzayın genişlemesi ve büyümesine katkı sağlamaktadır.

Siber güvenliğin ve siber alanın son yıllarda gelişmesine rağmen bunun bir başlangıç olduğu bir gerçekliktir. Teknoloji ile birlikte siber uzayın doğası da sürekli olarak gelişmekte ve literatüre yeni kavramlar eklenmektedir. Siber ile ilgili tanımlamaların ve ifadelerin kavramsallaşması, teknik bilgi gerektiren oldukça zor bir süreçtir. Siber uzay, interaktif ve etkileşimli bir alan olup kullanıcılar ondan yararlanmakla birlikte ona katkı da sağlamaktadır. Bu sebeple siber uzay ve siber güvenlik ile ilgili kavramlar ve literatür sürekli değişmekte ve gelişmektedir.

2.3: Siber Uzaya ve Siber Güvenliğe Kuramsal Yaklaşımlar

Siber güvenlik anlayışının kuramsal temelleri, uluslararası ilişkiler teorileri içerisinde gelişen güvenlik yaklaşımlarından hareketle oluşturulabilir. Siber ile sosyal bilimler arasında olan ilişki genellikle sorunlu olmuştur. Bunda sosyal bilimcilerin uzun zaman siber çalışmaları göz ardı etmelerinin yeri büyüktür. Siber alanı daha çok teknik bir disiplin olarak yorumladıklarından kodlar, programlar ve yazılımlardan ibaret bir alan sanmışlardır. Hâlbuki siber alanın sosyal, ekonomik ve hatta siyasal boyutu olup sosyal bilimciler tarafından da incelenmesi gereken bir alandır. Siber güvenlik anlayışının temellerinin anlaşılması idealizm, realizm, neorealizm gibi kuramsal yaklaşımlarca incelenmesi gerekmektedir.

İdealizme göre insan doğası iyi olup yardıma ve iş birliğine yatkındır. Doğru bir hukuksal düzenleme yapılırsa insanın kötü ve çatışmacı kimliği ortadan kalkacaktır. Bu sebeple kaosun engellenmesinin ve uluslararası güvenliğin sağlanmasının en etkili ve yararlı yolu, uluslararası hukukun tesis edilmesi ve hukukun uygulanmasını sağlayacak uluslararası örgütler kurmaktır (Karabulut, 2015: 52-54).

Realist düşünürlere göre güç ve güvenlik arasında doğrusal ve paralel bir ilişki vardır. Bunun anlamı ne kadar güç elde edilirse veya güç biriktirilirse o kadar güvenlik elde edilecektir. Bu güç birikiminin temel amacı barışı sağlamlaştırmaktır. Bu sebeple devletlerin siber güvenliklerini oluşturmalarının temelinde siber güvenliklerinin arttırması gelmektedir. İdealizm bakış açısına göre ise siber güvenliğin sağlanması için karşılıklı yardıma ve iş birliğine ihtiyaç duyulmakta olduğu savunulabilir.

Neorealist güvenlik anlayışına bakıldığında Kenneth Waltz'ın analizlerine bakılması gerekir. Waltz, devletlerin uluslararası politikada esas aktör olduğunu kabul etmekle birlikte sistem olarak analiz

yapmaya çalışmıştır. Uluslararası siyasi yapıyı incelemiştir. Waltz, analiz düzeylerinin ilişkisi yerine uluslararası sistemin yapısal bileşeninin nasıl olduğuna odaklanmıştır. Güç dengesinin düzen anarşik olursa ve varlığını sürdürmek isteyen birimler olursa geçerli olacağını savunur. Bu sebeple iki kutuplu düzenin üç ve daha fazla kutuplu düzenden daha istikrarlı olduğunu savunur (Griffiths, Roach, Solomon; 2011: 58-60).

Soğuk savaş sonrası güvenliğe genel olarak bakış açılarında değişiklikler olmuştur. İdealizmin "barışı tesis etme" bakış açısı, realizmin "güç" temelli bakış ve neoralizmin "anarşik güç dengesi" merkezli bakış açıları eleştirilmeye başlanmış ve günümüz dünyasını açıklamada yetersiz kaldığı ileri sürülmüştür. Geleneksel güvenlik anlayışları tam anlamıyla reddedilmemekle birlikte siber güvenlik alanında bakış açısı oluşturma anlamında temel olmuş, düşünmeye ve tartışmaya zemin hazırlamıştır.

1970'lerde başlayan geleneksel güvenlik anlayışlarına yönelik tepkilerle birlikte güvenlik kavramının yeniden sorgulanması gerekliliği ortaya çıkmıştır. Bunun iki önemli nedeni olmuştur; Soğuk Savaşın bitmesi ve küreselleşmenin uluslararası ilişkilerin her alanını etkilemesidir (Karabulut, 2015: 78-79).

Özellikle 1970'li yıllarda ortaya çıkan ve devlet odaklı analiz yapan düşünce okullarına karşı tepki olarak doğan Plüralizm, artan karşılıklı bağımlılık ve karşılıklı etkileşim sebepleriyle geleneksel güvenlik anlayışına tepki olarak çıkmıştır (Arı, 2011: 331).

Güvenlik çalışmalarında özellikle Amerikan egemenliğine alternatif olarak çıkmış olan Kopenhag Okulu, literatüre "güvenlikleştirme", "güvenlik sektörleri" gibi birçok kavram kazandırmış olup, güvenliği ekonomik, politik, çevresel, toplumsal ve insani güvenlik sektörleri olarak incelemiştir. Özellikle geleneksel devlet merkezli güvenlik anlayışına eleştiri olarak çıkan Eleştirel güvenlik anlayışı, bireylerin de çalışılması gereken konular olduğunu söylemektedir. Sosyal İnşacı, Feminist ve Post-modern teorilerde de devlet merkezli güvenlik anlayışına eleştiri vardır (Goyushov, 2019: 697).

Güvenlikleştirme eylemi, güvenlikleştirici olan bir konuyu ele alıp güvenlik tehdidi olarak algılayarak olağan üstü tedbirler almaktadır. Başarılı olarak adlandırılan bir güvenlikleştirme ise, hedef kitlenin konuyu tehdit olarak görüp konunun bir güvenlik sorunu olarak kabul edilmesiyle mümkündür (Baysal ve Lüleci, 2015: 76). Siber güvenlik pek ala güvenlikleştirilip olağan üstü tedbirler alınabilir, internette yasaklamalar getirilerek yapılabilir olsa da onun vatandaşlar ve dinleyiciler tarafından bir tehdit olarak algılanması da gerekmektedir.

Kopenhag Okulu ekolüne göre güvenlikleştirme kavramı ile değer verilen bir şey tehdit olarak tanımlanarak yeniden inşa edilir ve sonrasında askeri tedbirler de dahil olmak üzere üst düzey önlemler alınabilir.

Siber güvenliğin güvenlik-dışına ötelemek mi yoksa güvenlikleştirilmesi ve önlemler alınarak tehdit sıralamalarında üst düzeye çıkarmak devletlerin politikalarına bağımlı olsa da politika yapıcıların tehdit ve risk algılama düzeylerine göre değişkenlik göstereceği aşikârdır. Çünkü politika yapıcılar ve karar alıcılar belirleyici olduklarından siber anlamında bilinç düzeylerinin danışmanları da dâhil olmak üzere arttırılması gerekmektedir.

Günümüzde siber güvenlik önemli hale gelmiş olduğu tartışılmaz bir gerçeklik olup siber alandan ve teknolojik gelişmelerden geri kalınmaması için güvenlik politikalarını bu bakış açısıyla oluşturmak gerekmektedir. Güvenlik teorilerinin bakış açılarında siber güvenliğe ve güvenliğin nasıl tesis edilmesi gerektiğine bakışı paralellik göstermekte olup özellikle 1970'ler ile güvenlik kavramının yeniden sorgulanmasıyla daha çok gündeme gelmiştir. Özellikle siber güvenliğinde Türkiye için "aciliyet" kapsamına alınıp ciddi tedbirler alınması elzemdir. Siber güvenliğin güvenlikleştirilerek tedbir alınması

bu konuda yetişmiş eleman ve altyapı geliştirilmesi gerekmektedir.

2.4. Siber Uzayda Çatışma ve Ulus Devletlerin Siber Savaşı

Devletler, siber saldırıları askeri bir çatışmaya gerek olmadan kullanılabilecek bir yöntem olarak görebilmektedirler. Siber uzayda saldırganın kimliğini gizleyebilmesi ve işlenen-yapılan siber suçun tespit-isnat (attribution) konusunun karmaşık olması sebepleriyle devletlere cazip hale gelebilmektedir (Darıcılı, 2018: 324).

Günümüzde ulus devletlerarasında siber savaş tehdidi yeni tehdit olarak algılanmaktadır. Ancak siber savaşlar tarihsel olarak birçok kez gerçekleşmiştir. Bunlardan bilinen en dikkat çekici olanı casus program olan Promis'tir. Promis konusunu ele alan dosyalarda Dünya Bankası ve Uluslararası Para Fonu (IMF)'nun, CIA(ABD Merkezî İstihbarat Teşkilatı) ve MOSSAD yararına bilgi sızdırdığı ileri sürülmüştür. ABD'nin bu tip program aracılığıyla hedef ve rakip ülkelerin banka sistemlerini kilitleme ve kontrollü mali krizlere yol açtığı ileri sürülmüştür (Kuzu, Ağustos 2019:188-189).

Gelecek dönemlerde bilgisayar ağlarına siber saldırılar, askeri operasyonlar için mühimmatların veya araçların sahaya ulaştırılması kadar önemli hale gelecektir. Askeri operasyonların önemli özelliğinde bilgisayar ağlarına saldırlar ve siber savaş yer alacaktır. 1995 yılında Çin Ordusu finans sistemlerine saldırıyı yararlı bir asimetrik silah olarak değerlendirip 1997 yılında "Bilgisayar Harbi" olarak tatbikatlar yapmıştır (Kuzu, Eylül 2019: 24).

Çinli uzmanlar, bilgisayar virüsleri ile hedef sistemleri izlemek ve yönlendirerek rakip füzelerinin kendine geri döndürerek kullanabileceğini ifade etmişlerdir. Çinli güvenlik uzmanlarınca bir bilgisayardaki bir gram bütünleşmiş devre sistemi bir ton uranyumdan daha faydalı olabilmektedir (Kuzu, Eylül 2019: 24).

11 Eylül sonrasında uluslararası arenada en çok konuşulan meselelerden biri NATO üyesi olan bir devlete gerçekleştirilebilecek siber saldırı ya da "Dijital Felaket" (diğer adı dijital 9/11) senaryosuydu. Muhtemel bir dijital Pearl Harbour beklentisi artmıştı. Devletlerin siber sistemlerine saldırı ile kritik alt yapıları ve ekonomisine ciddi zararlar verilmesi ve bunun güvenliklerini sarsacağı korkusu gelişmiştir. Bu korku sebebiyle birçok ülke ulusal güvenlik belgelerine siber güvenlik stratejilerini eklediler (Bıçakçı, 2014: 119).

Siber terörizmi ciddi ve önemli bir tehdit olarak yaşayan en ilginç örneklerden biri Estonya'dır. Soğuk Savaşın sona ermesi ile birlikte Rus kökenli vatandaşlarının artışı ile Ruslarla Estonlar arasında gerginlikler ve çatışmalar vardı. Rusya kaynaklı internet site ve forumlarında Estonya'daki adresler hedef gösterilmiş ve birçok siber saldırılar yapılmıştır. Estonya Savunma Bakanı, NATO teşkilatına ve NATO üyesi ülkelere yardım talebinde bulunmuştur. Uluslararası güvenlik anlamında Estonya'ya yapılan siber saldırılar bir milat-başlangıç oluşturmuştur (Bıçakçı, 2014: 119-121).

2015 tarihinde Rus Hacker grubu olan CyberBerkut, Alman Parlamentosu ve Şansölye olan Angela Merkel'in internet sitelerine saldırılar gerçekleştirmiştir. Siber saldırılar sadece web sayfalarına erişim engeli ile kalmayıp yaklaşık 20.000'i bulan politikacılara, destek personeli ve memurlara ait bilgisayarlara erişim ve veri akışı sağlamıştır (Eren, 2017: 62).

Avrupa Birliği'nin siber saldırılar ile siber güvenliğin önemi ile yüzleşmesinde Estonya saldırıları ve Alman Parlamentosuna saldırılar kadar bir başka referans kaynağı TV5 Monde Örneğidir. TV5 Monde siber saldırısını IŞID örgütü üstlenmiş olup kanalın Facebook ve Twitter hesaplarına da saldırı düzenlenmişti. Konu ile ilgili Paris Savcılığı siber saldırılar ile "Terör soruşturması" açıldığını duyurmuştur (www.bbc.com).

2015 yılında Paris'te Fransız dergisi olan Charlie Hebdo'ya gerçekleştirilen silahlı terör saldırı sonucunda 12 kişi hayatını kaybetmiştir. Saldırı sonrasında Anti-İslamcı yaklaşımlar sergilenmiştir. Sonrasında radikal İslamcı grup olarak bilinen CyberCaliphate TV5 Monde'ye siber saldırılar gerçekleştirmiştir. Kanal hizmet veremeyecek duruma gelip web ve sosyal medya hesapları da ele geçirilmiştir. TV5 Monde örneği devlet dışı aktörlerin de iyi bir şekilde organize olup siber saldırılar yapabileceğini göstermiş ve Avrupa Birliği'nin bu saldırılarla mücadelede yetersiz kaldığını ortaya çıkarmıştır (Eren, 2017:663-64).

Bireysel hakların sınırları ve meşru hükümet müdahalelerin sınırlanması hakkında uluslararası ve ulusal tartışmalar süregelmiştir. Wikileaks olayı davasında, hassas ve hükümetlerin gizli dokümanlarının yayınlanması sonrası gizli belgelere erişilmesi sebebiyle ağır bir suç olarak yargılamalar yapılmıştır. Bazı Avrupalı ülkeler başta olmak üzere Wikileaks internet adresine erişim yasağı getirmiş olsa da bu bilgilere birçok kişi erişebilmiştir (Bendiek, 2012:8).

Wikileaks olayı davası devletlere siber güvenlik tedbirleri alınmazsa gizli kalması gereken belgelerin ifşalanması sebepleriyle çok zor düşülebildiğini göstermiştir. Özellikle Avrupa Birliği, NATO veya uluslararası kurumlardan ziyade en temelde devletlerin kendisinin önlem almasını gerçeğini ortaya çıkarmıştır.

Avrupa Birliği üye ülkelerde siber güvenlik politikaları minimum düzeyde standartlar getirmiş olsa da haksız yere bireysel hakları ihlale ve demokratik ilkelere aykırı düzenlemelere izin vermemektedir. Birliğe üye devlet önce kendi siber güvenliğini almalı ki Avrupa Birliği siber güvenliğine katkı yapabilsin. Demokratik ilkeler gözetilerek oluşturulan bir siber güvenlik politikaları oluşturulmaya çalışılmakla birlikte, Birlik güvenliğine zarar gelmemesi için belirli bir birliktelik sağlaması açısından önemli bir aşama kaydetmiştir. Üye ülkeler hem kendi ulusal düzenlemelerini hem de uluslararası düzenlemeleri yapması gerektiği için çok katmanlı küresel bir politikayı ifade etmektedir. Birliğin içinde özel güvenlik şirketlerinin de bu politikalarda etkin bir rol almaya çalıştığı da görülmektedir. Enerji, sağlık, ulaşım şirketlerinin bu yapıda yerini alacağı kuşkusuzdur. Avrupa Birliği siber güvenlik politikaları iyi yönetişim olarak formüle edilen şeffaflık, hukukun uygulanması, sorumluluk ve ortak yönetim ilkeleriyle hareket etmektedir (Bendiek, 2012:5-6).

Dünya da bilinen büyük hackerlarından biri olarak bilinen ve tutuklanmış Kevin Mitnick ABD'de gizli şirket bilgilerini çalmış ve Amerikan Ulusal Güvenlik ağını çökertmiştir. Bir başka hacker Jonathan James daha henüz 16yaşında iken NASA'nın sistemine girmiş ve 1.7 milyon Amerikan doları değerinde program/yazılım indirmiştir. Tüm bu eylemlerin arkasında terörist örgüt veya devlet olmadan gerçekleşse de devletin savunmasına tehdit olmak isteyenler için örnek alınabileceğinden güvenlik anlamında önemlidir (Çakmak ve Altunok, 2009: 89).

Rusya, kendi kontrolünde bulunan ancak belirli bir kuruma bağlı olmayan ve bağımsız hacker gruplarının siber güvenlik alanındaki faaliyetlerini ve eylemlerini desteklemektedir. Rusya siber güvenlik alanında etkili politikalar geliştirmiş ve siber alanda sayılı ülkeler arasına girmiştir. Ayrıca siber güvenlik politikalarını geliştirip yaygınlaştırmasıyla Rusya dış politika çıkarlarında kazançlı çıkmış ve bundan çok kez olumlu anlamda yararlanmıştır (Acar ve Pekcandanoğlu, 2020: 166-167).

Rusya siber güvenlik politikalarını 1994 yıllarında gözden geçirme kararı vermiştir. Buna sebep olan olay ise 1994 Rus-Çeçenya arasında geçen savaştır. Çeçenler bu savaşta bilgi teknolojilerini çok iyi kullanmışlardır. Çeçenler kendi self-determinasyon hakkını ilan ederken ve Rusya'nın insan haklarını ihlal ettiğini belgelerle ilan ederken Batı'ya çok iyi propaganda yapmışlardır. Böylece Rusya savaş

stratejilerinde büyük değişikliğe gitmiş ve Medya organizasyonlarını, görsel ve yazılı teknolojiyi kontrol altına almaya çalışmıştır (Acar ve Pekcandanoğlu, 2020: 169).

Günümüzde ulus devletler bilgisayar korsanlığı ve siber güvenliklerini sağlamak amacıyla hackerler yetiştirmekte veya kullanmaktadırlar. Sadece kendi güvenliklerinin sağlanması konusu değil rekabet etme amacıyla da etkinliklerini arttırmaya çalışmaktadırlar. Bu sebeple hacker olarak bilinen gençleri çıkarları gereği kullanan Rusya, uluslararası camia da dikkat çekmiştir.

Rusya 2007 Estonya, 2008 Gürcistan ve Litvanya, 2009 Kırgızistan ve 2014 Ukrayna ile olan savaşlarında Siber saldırı kapasitesinin arttığı görülmüştür. Örneğin Estonya'nın Parlamentosu başta olmak üzere bankaları, siyasi parti siteleri, telekomünikasyon şirketlerinin hacklenmesinde Rus Hackerler başarılı olmuşlardır. Daha sonra Estonya'nın NATO ve ABD'den destek alması ve siber güvenlik önlemlerini alması süreci siber güvenliğin önemini göstermiştir (Acar ve Pekcandanoğlu, 2020: 179-180).

Rusya'nın dış politika problemlerinin çözümünde de siber saldırıları ve sabotajları bir argüman olarak sunması ve masada bir tehdit seçeneği olarak göstermesi yeni tip bir mücadele alanını ortaya çıkarmıştır. Rusya'yı tehdit olarak gören tüm ülkeler Rusya tarafından siber saldırılar düzenlenebileceğine yönelik tehdit algısı algılayıp bu alanda güvenliklerini arttırmaya ve tedbir almaya çalışmışlardır.

2014 yılında NATO üyesi devletler siber savunmayı genel savunmanın ayrılmaz bir parçası olduğunu vurgulamış olup 5. Maddenin kullanılabileceğini belirtmişlerdir. 2016 yılında siber tatbikatlar yaparak siber savunmalarını güçlendirmeye söz vermişlerdir. Ayrıca ittifakın genel politikası bir üye devletin diğer üye devlet kadar yetenek sahibi olması şart ve zorunludur. İttifak ve müttefiklerin yaptıklarının yeterli olup olmadığı tartışmalı olmakla birlikte siber savunma konusunda ittifak ve üyeler önemle üzerinde durmalıdırlar (Brent, 2019, NATO'nun siber uzaydaki rolü, www.nato.int).

NATO'nun siber saldırıları güvenlikleştirip tehdit boyutunu arttırması NATO kuruluş anlaşmasındaki 5. Madde ile ilişkilendirilmiş olup tehdit algıları yeni bir boyut kazanmıştır. Bu siber güvenlik tedbirlerinin alınması, konuya önem verilmesi, harekâtların senkronize olması ve her şeyden önemlisi bilgi paylaşılması açılarından katkı sunduğu söylenebilir.

Kara, deniz, hava ve uzaydan sonra siber savaşı harbin beşinci boyutuna geçilmiştir. Savunma ve radar sistemleri başta olmak üzere, İnsansız hava araçları, internete bağlı veya internete bağlı olmayan kapalı devre sistemlere sahip siber araçlar, füzeler, nükleer sistemler siber savaşların olması durumunda yıkımların ne boyutlarda olabileceği hakkında bilgi verebilmektedir. Yıkımların çok ağır olmaması adına siber güvenliği yakından takip etmek gerekmektedir. Özellikle siber güvenlik ile alakalı yenilikler ve teknoloji takip edilmelidir. Aksi halde takipten geri kalınırsa onarılmaz zararlar ve teknolojik gerilik ile karşılaşılacaktır. Teknoloji ve siber güvenlik literatürü takip edilemezse her türlü siber tehlikelere açık olunacak ve saldırılar kaçınılmaz olacaktır. Özellikle bu saldırıların askeri ve ekonomik sonuçları çok ağır olacaktır.

Çin ve ABD hackerlarının siber savaşı ve siber yüzleşmesi olarak bilinen ve 'Birinci Siber Dünya Savaşı' olarak adlandırılan 2001 yılında gerçekleşen saldılar birçok devleti etkilemiştir. ABD keşif ve casus uçağı Çin jeti ile çarpışması sonucu Çin ve ABD hackerları saldırılar düzenlemiştir (Cavelty, 2015: 408).

Siber suçların sonuçları bireyler kadar kurum, şirket veya devletleri de etkileyebilmektedir. Bu sebeple siber suçların küresel olarak tartışılma boyutu etkilediği aktöre göre değişkenlik gösterebilmektedir. Klasik bir terör faaliyetinde silah ve bomba kullanılması ile belli bir bölge, alan veya insanlar zarar

görürken siber terör faaliyetlerinde bilgisayar ve bilgi sistemi kullanılması marifetiyle devlete ekonomik, sosyal ve siyasal sonuçları büyük ölçüde ve milyonlarca kişiyi etkileyebilecek zararlara sebep olabilmektedir. Üstelik terörü kontrol altına alma veya minimize etmek mümkün iken siber terörist grupları ve hackerları tespit ve yok etmek çoğu zaman imkânsızdır.

Devletler bu sebeplerle analizcisinden büyük veri yöneticisine, programcısından yazılım geliştiricisine kadar gerekirse fiziksel ordusu gibi bir bilgi teknoloji (IT) ordusu kurması artık günümüzde zorunluluktur. Devletlerin petrol, doğalgaz veya nükleer santral kurması kadar artık güçlü bir bilgi sistemi ve alt yapısının kurmasının önemi artmıştır.

3. SİBER HUKUK VE SİBER SUÇLAR

İnsanoğlunun tarihsel gelişimine bakacak olursak avcı toplayıcılıktan yerleşikliğe geçip tarım çağına geçmiştir. Tarım çağı sonrası sanayi çağına geçen insanoğlu günümüzde bilimin ve teknolojinin gelişimi ile birlikte bilgi çağına geçmiştir. Bilgi çağına geçerken insan haklarının tarihsel gelişimi de sürmüştür. İnsan haklarının tarihsel gelişimi insanlığın gelişimi kadar önem arz etmektedir. İnsan haklarının tarihsel gelişiminde en önemli şey iktidarın veya egemen olan kralın yetkilerinin sınırlandırılması meselesi vardır. Böylelikle insan hakkına ve özgürlüğüne dokunulmayarak düşünsel ve tarihsel olarak gelişme göstermiştir.

İnternetin hayatımıza girmesiyle insan hakları yeni bir mecraya ve alana taşınmıştır. Bu sebeple yeni düzenlemeler yapılması ve bazı hakların daha çok korunması veya müdahale edilmemesi gerekliliği doğmuştur. Örnek olarak dijital çağa uygun olmayan vergi sistemi getirilirse internet üzerinden alışverişlerde vergi usulsüzlükleri olabilir veya dış ticaretin büyük çoğunluğu günümüzde internette geliştirildiği için dış ticarette vergi adaletsizliği önlenemezse bu da insan haklarına aykırı olabilir. Bir başka örnek olarak insanların internet sitesine erişim hakkının engellenmemesi gerekmektedir. Haberleşme özgürlüğüne saygı duyulmalı ve gereksiz kısıtlamalar yapılmamalıdır. Bir başka örnek olarak internetten alışveriş yapılırken güvenli yapılabilmeli ve bunun yanında kişisel verilerinin üçüncü şahıslarla paylaşılmamasını isteme hakkına sahip olunmalıdır.

İnternet yoluyla işlenen siber suçların ve hak ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir. Bu ihlallerin toplum üzerindeki etkisi yadsınamaz. Siber zorbalık, yetkisiz erişim, özel hayatın gizliliğini ihlal, internette çocuk istismarı, banka bilgilerinin ele geçirilmesi ve diğer siber suçlar internet yoluyla gerçekleşen insan hakları ihlalleridir. Bu ihlallerin önlenmesi ve yaptırımların da etkili olması gerekmektedir.

Hukuk dinamik olup sosyal, kültürel, siyasal boyutları olmaktadır. Siber hukuk ta dinamik olup bunlardan bağımsız olamaz. Her ülke kendi örf ve kültürü, teknolojik gelişme düzeyi ve yaşama standartlarına göre siber hukuk anlamında düzenlemelere gitmiştir. Her ülkenin siber suç tanımları ve yaptırımları farklıdır. Bir ülkeye göre siber suç olabilecek bir eylem başka bir ülkeye göre olmayabilmektedir. Ayrıca siber suç kabul görülen eylemlerin yaptırımları ve infaz rejimleri de farklı olabilmektedir. Küresel bir anlaşma veya ortaklığın olmaması bir yana siber suçlar üzerinde bile anlaşma veya uzlaşma yoktur. Durum böyle iken ulusal düzenlemelerin yetersiz kalacağı açık olup uluslararası veya sınır aşan suçlarda etkili çözümler elde edilememektedir.

Siber suçlar bir "şiddet eylemi" olarak kullanılabilmektedir. Bu sebeple toplumsal, psikolojik ve duygusal olarak insanları ciddi boyutta etkilemektedir. İnsanların birbirlerine yaptıkları zorbalıkların veya suçların internet vasıtasıyla siber ortamda yapılmasıyla karşımıza "siber zorbalık" kavramı çıkmaktadır. Siber zorbalık olarak literatürde çok çeşitli tanımlamalar vardır. Genel kabul görmüş

bir tanım olmamakla birlikte teknoloji aracı kılınarak gerçekleştirilmesi ve zorbalık veya zarar verici rahatsız eylemler olmasında ortaklaşmış olduğu görülebilir.

Siber zorbalığı, akran zorbalığından yaygın olmasının en büyük sebeplerinden birisi yüz yüze olmaması ve sanal ortamda gerçekleşmesidir. Özellikle failin veya şüphelinin takma hesap-anonim hesap ya da sahte hesap kullanılarak yapılması ve gerçek kimliğin gizlenmesi zorbalık yapmayı kolaylaştırmaktadır. Durum böyle iken mağdur ve mağdurun çevresine etkisi çok büyük olabilmektedir. Failin kimliğinin tespitinin zor olması mağdurun psikolojik şiddete daha fazla mazur kalmasına sebep olmaktadır.

Teknoloji ve bilimin ilerlemesiyle özellikle günlük hayatta insan yaşamını kolaylaştırmıştır. Ancak teknolojik araçların insan hayatında çok fazla kullanımı, mahremiyet hakkının ihlal edilebileceği konusunda kaygılar doğurmuştur. Sağlıklı bir şekilde kullanılmayan teknoloji topluma zarar getirir. Eğer yasalar ile denetlenmezse sadece kişinin ruh veya fiziksel sağlığını değil toplumun bütünlüğü ve barışını tehlikeye düşürebilecektir. Günümüzde internet üzerinde kişilik hakkına saldırı çok kolay hale gelmiştir. Ayrıca basın, televizyon, haber siteleri ve sosyal medya yolu ile geniş kitlelere kolayca kısa zamanda ulaşılabilmektedir. Bir internet sitesinde özel hayatın gözler önünde olması ve gerçek dışı olan yayınlar ile şeref ve haysiyeti zedeleyici ihlaller olup internette kişilik hakkı ihlallerindendir. İnternet yoluyla işlenen İnsan hakları ihlallerinin olmaması için hem kamu sektörü hem özel sektöre önemli görevler düşmektedir.

Devletin yanı sıra birçok kurum ve kuruluş bireyler hakkında bilgi toplayarak özel hayatın gizliliğini ihlal etme imkânını bulabilmektedirler. Örnek vermek gerekirse özel veya kamu hastanelerinde parmak izi kaydı alınması, GSM operatörlerinin reklam için veya bir başka sebeple kullanıcısı olmayan bireylerin telefonuna ulaşıp ürün veya reklam tanıtımı için arama yapması, özel ve kamu iş yerlerinde kameralar ile denetim gibi birçok örnek verilebilir. Yapılacak düzenlemelerinde sadece kamuyu değil özel kurumları ve kuruluşları da içerecek şekilde düzenlemeler yapılması gerekir.

Teknolojinin suç işlemeyi kolaylaştırdığı gerçeği de göz ardı edilmemelidir. Suçlular, suç işleme ve işledikleri suçları gizleme konusunda teknolojik yeniliklerden faydalanmaktadırlar. Bu sebeple suç ve suçlularla mücadelede güvenlik güçlerinin başarılı olabilmesi için teknoloji ve teknik donanım kullanımı tercih değil zorunluluk meselesi olmuştur.

Güvenlik ve emniyet güçlerinin teknolojiyi kullanacak personellerine gerekli profesyonellik eğitimi vermesi gerekmektedir. Ayrıca bu profesyonellik eğitimi yanı sıra meslek etik ve ahlakı da verilmesi gerekmektedir. Aksi halde gerekli eğitim ve kültür verilmediğinde teknolojiyi kullanan personel keyfiyet için veya kendi çıkarı için teknoloji ve yetki aşımı yapabileceklerdir.

M.Foucault' a göre hapishanelerin, ıslahevlerinin, tımarhanelerin amacı sadece güvenliğin sağlanması değil aynı zamanda toplumda disiplin mekanizması işlevi göstermesidir. Hapishaneler özellikle işçi sınıfının denetlenmesinde ve bir disiplin müessesesi gibi "hapishane takımadası" oluşturulmuştur. Sakinlerini gözetleyerek, topluma tehdit oluşturmayacak "uysal bedenler" yapmayı hedefliyordu (Zedner, 2015: 39-40).

Herkesin gözetim ve denetim altında olduğu büyük hapishanede olduğu gibi düşüncesi bir tür paranoya dönüşse de teknolojik imkânların kullanımı ile birlikte artan bir şekilde gözetleme ve kayıt altına alma devam etmektedir. Bunun paranoya boyutuna dönüşmeden gerekli yetki ve düzenlemeler yapılırsa ortadan kaldırabileceği açıktır.

Siber Suç tanımına bakılırsa, bir bilişim sisteminin güvenliğine ve bu güvenliğe bağlı verileri ve/veya

kullanıcısını hedef alan ve özellikle de bir bilişim sistemi vasıtasıyla işlenebilen suçlardır (https://www.egm.gov.tr).

Siber suç, bir bilişim sistemi kullanılarak işlenmekte olduğu bilinmektedir. Teknolojinin gelişimi ile birlikte artık tüm suçların bilişim sistemi kullanılarak işlenebileceği görülmektedir ancak her bilişim sistemi kullanılarak işlenen suçun da siber suç olmayacağı unutulmamalıdır. Siber suçlara literatürde bilgisayar suçu, internet suçu, internete özgü suçlar veya bilişim suçları gibi adlandırmalar yapılmaktadır. Birçok suç bilişim sistemi kullanılarak işlenebilir. Ancak yukarıda da dikkat edileceği üzere bilinmesi gereken siber suçu diğer suçlardan ayıran en önemli özellik bilişim sistemi kullanılarak işlenmesidir.

Teknolojinin gelişmesiyle suçlular her türlü teknolojik gelişmeden yararlanmaktadır. Örnek vermek gerekirse tam anlamıyla bir siber suç olmayan ancak bilişim yoluyla işlenen asayiş suçları vardır. İntihara Yönlendirme (TCK madde 84), Tehdit (TCK madde 106), Şantaj (TCK madde 107), Hakaret (TCK madde 125), Fuhuş (TCK madde 227), Kumar Oynanması İçin Yer ve İmkân Sağlama (TCK madde 228) gibi suçlar asayiş suçları olup bilişim yoluyla ve teknolojik imkânları kullanılarak işlenebilmektedir. Günümüzde her suç teknolojik olarak işlenebilmektedir. Terör örgütü propagandası ile terör suçu işlenebilecekken Cumhurbaşkanına hakaret (TCK madde 299), Devletin egemenlik alametlerini aşağılama (TCK madde 300) veya Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (TCK madde 301) ile devletin güvenliğine karşı suçlarda bilişim yoluyla ve teknolojik imkânları kullanılarak işlenebilmektedir.

Günlük hayatta olan suçlar ve suç tipleri dijital ortamda da görülmektedir. Kredi kartı dolandırıcılığı, banka hesabından izinsiz para harcanması, internette yasa dışı yayınlar, çocuk pornografisi, sosyal medya hesabın hacklenmesi, şirket veya kurumsal bilgisayarların sunucularının hacklenerek sonrasında fidye istenmesi, siber zorbalık faaliyetleriyle rahatsızlık verme çok sık karşılaşılan vakalardır. Sanal ortamda müstehcen yayınlar toplumsal ahlakı etkilemektedir. Tüm bunlar yasal bir düzenlemenin ve denetimlerin sağlam olmasını şart koşmaktadır.

Siber uzayın karanlık yüzü olarak adlandırılan Deep-weeb kısmında yasadışı faaliyetlerin olduğu sınırsız bir alanı ifade etmektedir. Uyuşturucu ticareti başta olmak üzere insan kaçakçılığı, kiralık katiller, çocuk pornosundan organize suçlara kadar birçok suçun işlendiği ve en az cezalandırıldığı alan olup büyük bir kısmı bitcoin ve sanal paralarla ticareti yapılmaktadır. Ulus devletler bunlarla mücadelede ise yetersiz kalmaktadır. Uluslararası işbirliğine ihtiyaç duyulduğunda ise devletlerin rekabet algısıyla hareket ettiği görülmektedir.

Mahremiyet hakkının ihlali konusunda genellikle devletlerin rollerine odaklanılır. Ancak günümüzde özel kişi ve kuruluşlar tarafından da özel yaşam alanına veya mahremiyet alanına tehditler olmaktadır. Siber uzay çağında mahremiyet alanının korunması için güncel hukuki düzenlemeler yapılması gerekmektedir. Günümüzde telefon görüşmelerin dinlenmesinden, kişisel elektronik posta ve maillerin okunmasından, kişisel bilgi ve fotoğrafların gazete sayfaları, televizyon veya internet sitelerinde paylaşılmayacağından, kişisel mali durumlarla ilgili bilgilerin başka kişi veya kuruluşlara pazarlanmayacağından emin olunmamaktadır (Yüksel, 2003:183).

Mahremiyet hakkı, klasik haklardan olan birinci kuşak haklardandır. Bu hakların en önemli özelliği bireyi koruması ve devleti sınırlandıran negatif statü haklarındandır. Bu haklar kişinin devlet, toplum ve üçüncü kişilerin dokunamayacağı özel alan yaratmaktadır (Fırat, 2015: 105).

"İnternette ifade özgürlüğü" kavramı yeni çıkmış bir özgürlük değildir. Mevcut olan bir insan hakkının yeni bir mecrada genişlemesi anlamına gelir. Aynı durum aslında internette anonim olma hakkında,

toplantı yapma ve dernek kurma özgürlüğü veya eğitim hakkı gibi özgürlüklerin internette kullanılması ve gerçekleştirilmesi için de geçerli olmaktadır (Benedek ve Kettemann, 2013:166).

İnternet mecrası yeni olsa da insan hakları tarihsel olarak çok eskiye gitmektedir. Bu açıdan düşünüldüğünde dahi insan haklarının yeni bir mecrada sürdürülmesi gerekmektedir. Ayrıca gelişerek devam eden insan hakları tarihi, teknolojinin insanlar arasında yaygınlaşması ile farklı bir şekilde kendini geliştirmek zorundadır. Artık insan hakları sadece fiziksel olarak insan hakkı ihlal edilmemekte, internet ve sanal ortamda da insan hakları ihlal edilebilmektedir. Bu sebeple insan hakkı ihlallerinin önlenmesi için gerekli düzenlemeler interneti de kapsayacak şekilde hukuki anlamda yapılmalıdır.

Son olarak devletlerin genel hatları ile siber hukuk anlamında yapabilecekleri ve yapması gerekli noktaları genel hatları ile maddeler halinde özet olarak belirtecek olursak:

- Her devlet kendi yasalarında geçen siber suçları güncellemeli ve mevcut yasalarını değiştirmesi gerekmektedir. Teknik bilgi ve teknolojiler geliştiği için suçlar da değişkenlik göstermekte, mağduriyet tipi ve oranları artabilmektedir.
- Devletler küresel oydaşma veya konsesüs sağlayarak bir hukuk sistemi oluşturmalılar. Bu mümkün gözükmüyor ise ikili veya çok taraflı anlaşmalar yaparak siber suçlara yaptırım konusunda mutabakat yapmaları gerekmektedir.
- Uluslararası örgütler, özel şirketler ve hükümet dışı kuruluşların da üzerine düşeni yapması için devletlerin politika geliştirmeleri gerekmektedir.
- Devletler savaş hukukunu ve insan hakları hukukunu geliştirmişken siber hukuk anlamında temel etik ilkeler geliştirmeli ve bunu yazılı hale dökmeleri gerekmektedir.

Uluslararası ilişkiler literatüründe ortak bir siber tanımı olmadığı gibi, ortak bir siber hukuk da bulunmamaktadır. Bölgesel olarak NATO ve Avrupa Konseyi gibi bazı kurumlar sınırlı olsa dahi işbirliği ve/veya anlaşmalar geliştirme başarısı gösterseler dahi, Birleşmiş Milletler nezdinde küresel düzeyde herhangi bir anlaşma yapılamamıştır (Akyeşilmen, 2018: 60-61).

Uluslararası ilişkilerde sadece devletlerin değil çok uluslu şirketlerin, hükümet dışı kuruluşların da gücü yadsınamaz. Bu sebeple uluslararası kuruluşların siber hukuka katkısı elzemdir. Örnek olarak Facebook milyonlarca kullanıcısı olan bir şirkettir. Siber suçlarda devletler ile iş birliği yapması ve elindeki kanıt veya bilgileri paylaşma anlamında suçluların yakalanması ve suçların aydınlatılmasında tabiri yerinde ise "elini taşın altına koyması" beklenir.

İnsan haklarını dijital çağda korumak için sadece devletlerin değil, bireylerin ve özel şirketler üzerinde bağlayıcı olacak uluslararası bir düzene ve uluslararası anlaşmalara ihtiyaç vardır. Kısaca anarşik uluslararası düzenin doğasının üstüne çıkacak küresel bir yürütme organına ihtiyaç vardır. Siber uzay sınırsız, paydaşı çok olan, mesafelere sığmayan ve anarşik yapısıyla insan haklarının bir aktörce korunmasını imkânsız kılmaktadır. Siber uzayın tüm paydaşlarını içerecek kapsayıcı bir yaklaşım benimsenirse insan hakları korunabilecektir. Bu uluslararası hukukta yeni öznelerin çıkmasına, devletin egemenliğinin sorgulanmasına yol açacaktır (Akyeşilmen, 2018: 304-305).

Uluslararası Adalet Divanı, Uluslararası Ceza Mahkemesi, AHİM veya Avrupa Birliği Adalet Divanı ve diğer uluslararası yargı divanlarında siber saldırı suçunu işlemiş devletler hakkında ve hatta devlet görevlileri hakkında yargılamalar yapılmalıdır. Hüküm verildiği takdirde devletler çıkan sonuca ve yaptırımlara uluslararası hukukun getirdiği sorumluluk gereği uymalıdırlar.

4. SİBER SALDIRI

Siber saldırılara karşı güvenliği sağlamak için öncelikle siber saldırının anatomisinin bilinmesi gerekmektedir. Saldırının bilinmesi gerekir ki önlem alınabilsin. Saldırıya karşı savunma gücü arttırılması için teknik olarak hazır olmak şarttır. Saldırganların genel olarak yaptıkları belli başlı ortak çalışmalar vardır. Bunun en bilinen yöntemi ve ilk aşaması bilgi toplamaktır. Özellikle internette açık kaynaklarda edinilen en ufak bir bilgi dahi saldırgan için önemli olabilmektedir. Bu bilgiyi kullanarak başka bilgilere ulaşmak kolay başvurulan yollardan olup maliyeti yoktur veya maliyeti çok azdır.

Terörist örgütler tarafından siber faaliyetlerle eylem yapma çekici bulunur. Geleneksel terörist metotlardan az maliyetli oluşu, silah ya da patlayıcı temin etmek zorunda olmayışı, saldırganın kimliğinin gizlenebilir oluşu, özellikle hedef seçilebilecek noktaların (silahlı kuvvetler, kuruluşlar) fazla oluşu ve uzaktan kumanda edilebilir olması gibi sebepleriyle çekici olur (TASAM, 2004: 5-6).

Saldırgan açık arayarak sistem hakkında yeterli düzeyde bilgiye sahip olduğunda sistemin açıkları hakkında bilgi toplamak amacıyla tekrar internet araştırmasıyla bu iş için kurulan site ve formları tarar. Gereken bilgiye ulaştığında test saldırıları yapmaktan çekinmez ve hedefine ulaşana kadar çalışır.

Kendisini kamu görevlisi olarak tanıtıp, hattınızın veya cep telefonunuzun terör örgütü tarafından kullanıldığı, bu örgütten ve adının karışmaması için mağdurlardan para, altın ve kıymetli eşya istemeleri yaygın bir yöntem olup özellikle yaşlı insanları çok kolay kandırabilmektedir. Savcı, polis veya herhangi bir kamu görevlisinin para veya altın istemeyeceği unutmamalı bununla ilgili bilinçlendirici reklamlar ve seminerler verilmelidir.

Siber uzay yeni bir muhabere ve rekabet alanı getirmekle kalmamış, stratejik ve hassas bir konu haline gelmiştir. Savunma alanından ekonomiye, ticaretten sağlık alanına kadar birçok sektörde kritik alt yapıların korunması siber güvenliğin sağlanması açısından önemli hale gelmiştir. Sadece Türkiye değil hemen hemen birçok ülkeye siber saldırılar düzenleyen uluslararası hacker grubu olan Anonymous çok etkili olmuştur. Saldırılarını hizmet akışını engelleyerek (DDOS) yapmasının yanı sıra sistem açıklarını kullanarak gizli belgeleri çalmıştır. Sadece kamu sektörüne değil özel sektör kesimine de saldırılar düzenlenmiştir.

Siber saldırılar genellikle hacking faaliyetleri olarak bilinmektedir. Bilişim sistemlerine yetkisiz ve izinsiz erişimler olup hukuka aykırı ve sahibinin bilgisi ve/veya rızası dışında erişilmektedir. Birçok ülkede ve Türkiye'de suç olarak sayılmakta ve bu suçla birlikte başka suçların işlenmesine kapı açmaktadır (www.egm.gov.tr).

Siber saldırı çeşitlerinden ve hacking faaliyetlerinin en aktif ve fazla kullanılan yöntemlerinden biri Bot-Net ya da başka bilinen adıyla D-DOS saldırı türüdür. Bot-Net/ D-DOS saldırıları bir bilişim sisteminin erişilmesini engellenmesi amacıyla yapılır. İlk olarak zararlı yazılım yüklenerek ele geçirilmiş ve "BOT" olarak tabir edilen bilgisayar ve sistemlere komut verilerek istenilen web sitesi çok sayıda giriş isteği aldığı için başka kullanıcılara hizmet verememesi ve ulaşımının engellenmesi eylemidir. Genel olarak anlaşılması için verilen örnek aynı anda on kişinin girebileceği bir market kapısına on binlerce kişinin yığılması ve marketin hizmet verememesi örneği açıklayıcıdır. Ticari, siyasi ve terör amaçlarıyla yapılabilmektedir (www.egm.gov.tr).

Genel olarak siber saldırı yöntemlerinin bilinmesi tedbirlerin alınmasında ve güvenliğin arttırılmasında yararı olmaktadır. Siber suç, ağ veya bilgisayar sistemleri aracılığıyla bilgisayar veya ağ sistemlerine karşı işlenebilen suçlardır. Bilgisayar ile ilgili suçlar basit internet dolandırıcılığından başlayıp

sahteciliğe, programların telif haklarına aykırı olarak paylaşımı ve dağıtılmasına, Telekomünikasyon sistemlerinin çökertilmesine, internetten çocuk istismarına ve banka hesapları vurgununa kadar çok çeşitli olarak yelpaze de işlenebilmektedir.

Deprem bir doğal felakettir. Bu doğal felaket olmadan önce önlem alınması gerekmektedir. Siber saldırılar doğal olmasa bile bir felaket olarak bakılabilir. Dolayısıyla siber saldırılar olmadan önce de tedbirler alınması gerekmektedir. Eğer önlemler sağlam ve yerindeyse veri kaybı olmadan, sistem ve bilgiler zarar görmeden saldırı atlatılabilir. Acil durumlarda karşılık verme ve nasıl müdahale edilmesi gerektiği ve nasıl bir plan ve silsile izleneceği önceden oluşturulmalıdır.

Siber güvenlik anlamında en önemli öncelik sağlanması gereken konuların biri de tabiri doğru kullanmak gerekirse "virüslenmemek"tir. Bu bir internet sitesine girerek veya gerekli güvenlik önlemi almayarak kendi kendimize karşılaşabileceğimiz gibi bir hacker veya kötü niyetli kişi veya kişilerce sabotaj edilerek de karşılaşılabilmektedir. Bu konuda bizim sormamız gereken soru şu olmaktadır: Virüslendikten sonra acil müdahalemiz ne olmalı veya neler yapılmalı sorusu olmalıdır. Virüslendikten sonra ilk yardım ve acil müdahaleler önemlidir. Nasıl ki trafik kazasında acil müdahaleler gerekliyse virüslendikten sonra da acil müdahaleler "hayat kurtarıcı" olabilmektedir.

Özellikle bir acil güvenlik planı oluşturulurken daha önce eylem planı varsa eksikliklerine bakılması, eğer eylem planı yok ise sağlam bilgiye dayalı bir bilgi sistemine dayalı eylem planı oluşturulmalıdır. Her şeyden önemlisi ise siber saldırı olmadan önlem alınmasıdır. Aksi halde bir nükleer tesis kontrolden çıkabilir, elektrik şebekesi çökebilir, uydu sistemleri ele geçirilebilir, uçukların kontrol sistemi kaybedilebilir, metro veya tren kazalarına yol açacak siber güvenlik ihlalleri ile karşılaşılabilmektir.

Siber saldırılar önlem alınmazsa çok büyük zararlara sebep olabilmektedir. Doğalgaz hatlarına sabotaj düzenlenerek bir ülkeyi hem ekonomik hem de binlerce kişiyi mağdur edebilir. Nükleer sistemlerine zarar vererek işlemez duruma getirebilir veya büyük çevresel felaketlere sebep olabilir. Hava trafiği veya deniz seferleri aksatılarak binlerce kişi mağdur edilebilir. Askeri cihaz veya silahlara siber saldırılar düzenlenerek imha edilebilir veya kendi vatandaşlarına karşı terör eylemi gerçekleştirilebilir. Özellikle bankalara siber saldırılar düzenlenerek ciddi ekonomik zararlara sebebiyet verilebilir. Örnekler çoğaltılabilir. Bu sebeple devletlerin hem gerekli tedbirleri alması hem de uluslararası hukukun getirdiği sorumluluklara uygun davranması gerekmektedir.

5. TÜRKİYE'NİN SİBER GÜVENLİK FARKINDALIK DURUMU VE TÜRKİYE'NİN GÜVENLİK POLİTİKALARINA ETKİLERİ

Türkiye'nin resmi siber güvenlik kurumları temelde üç ana amaç çerçevesinde örgütlendirilmiştir. Bu ana amaçların ilk grubunda olanlar siber suçlarla mücadele edip istihbarı çalışmalar yapma amaçlanmaktadır. Bu kurumlar İçişleri Bakanlığına bağlı olan Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma ve Sahil Güvenlik Komutanlığı bünyesindeki birimlerdir. İkinci grupta olanlar ise Türkiye'nin kritik ve önemli altyapılarının siber güvenliğinin sağlayacak olan siber saldırı engelleme ve savunma kapasitelerini oluşturulmasıyla görevlendirilmiş BTK, TSK Siber Savunma Komutanlığı, MİT, TUBİTAK, AFAD gibi kurumlardır. Üçüncü grupta olanlar ise devlet destekli olan özel girişimlerdir. Bunlar ise; Savunma Teknolojileri Mühendislik, ASELSAN ve HAVELSAN bünyesindeki birimlerdir (Darıcılı, 2019: 28).

Türkiye de siber güvenlik olaylarına müdahale için ulusal ve uluslararası koordinasyon amacıyla USOM yani "Ulusal Siber Olaylara Müdahale Merkezi" kurulmuştur. Bu birim, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde oluşturulmuştur (www.btk.gov.tr).

BTK bünyesinde olan Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT), kendisine ulaşan ihbarları değerlendirerek tehditleri bertaraf etmek için çalışmaktadır. Gerekli gördüğünde Kamu Kurum ve özel kişiler ile ilgili koordinasyon kurar. İhbarların çözüm sürecine kadar takibini yaparak çözüm üretir ve gerekli gördüğünde siber güvenlik tatbikatları yaparak kamu kurumlarının ve kuruluşlarının siber saldırılara karşı farkındalığını geliştirmektedir (www.usom.gov.tr).

Bilgi Teknolojileri ve İletişim Kurumunun sunmuş olduğu "İnternet Bilgi İhbar Merkezi" hizmeti dikkate değerdir. Buna göre 5651 sayılı yasa uyarınca: İntihara yönlendirme, Çocukların cinsel istismarı, Uyuşturucu veya uyarıcı madde kullanımının kolaylaştırılması, Sağlık için tehlikeli madde temini, Müstehcenlik, Fuhuş, Kumar oynanması için yer ve imkân sağlanması, Atatürk aleyhine işlenen suçlar ile ilgili yeterli şüphe oluştuğu takdirde internet uzantılarını yazarak içerikleri, İhbar Web'e giriş yaparak şikâyette veya ihbarda bulunulabilmektedir (www.ihbarweb.org.tr).

Ulaştırma ve Altyapı Bakan Yardımcısı Ömer Fatih Sayan'ın ifadesine ve belirtmesine göre Türkiye'ye geçen yılda 150 bin siber saldırı gerçekleşmiş olup bu saldırılar bir önceki yılın iki katı olması dikkat çekicidir (https://www.aa.com.tr/tr/turkiye/turkiyenin-siber-saldirilari-onleme-merkezi-kapilarini-aaya-acti/1727981). İnternette saldırılar ve siber olaylar giderek artmaya devam edecektir. Bunun için hazır olunması gerekmektedir. Sadece yetişmiş insan gücünden değil vatandaşların bilinçlendirilip farkındalık çalışmalarının da artması gerekmektedir. Siber saldırıların önlenmesi için alt yapı çalışmalarının ve güvenlik önlemlerinin alınabilmesi için yeterli kaynak ve bütçelerinde ayrılması gerekmektedir.

Türkiye'nin siber güvenliğinin arttırılması için müdahale kabiliyetinin arttırılması gerekmektedir. Her kurum ve birimde teknoloji ile ilgili bir departman harici bir müdahale birimi olması, sızma testleri yapıyor olması ve uzman personelin güncel bilgileriyle görev yapması önem arz etmektedir.

Rusya, Çin ve Amerika Birleşik Devletlerinin siber güvenlik belgelerinde veya siber uzay alanındaki yatırımları ve planlamalarını açıkça belirtmekten kaçınmakta veya sınırlı bilgi vermektedirler. Türkiye'de bu tavra dikkat etmeli ve planlamalarını gerekirse müttefikleriyle dahi paylaşmamalıdır.

Türkiye'nin siber anlamında kendini geliştirmesinde önüne engel olan durumlar vardır. Özellikle jeopolitik öneminden kaynaklı askeri ve güvenlik alanına çok ciddi para harcanmaktadır. Bu sarfiyatın siber güvenlik kısmına ciddiyetle ve samimi aktarım yapılmalıdır. Özellikle iç politikada değişen sürekli gündemler ve politikalar, yapılması gerekenlerin önüne geçmemelidir.

Türkiye'nin güvenlik politikaları ve aldığı kararlar incelenecek olursa siber güvenliğe ve önemine yer verilmekle birlikte bunun yeterli olup olmadığı tartışmalı bir konudur. Özellikle diğer ülkeler incelendiğinde ya adımların yetersiz olduğu ya da alınmış olan önlemlerin ilan edilmemesi ve haberleştirilmediği için bilinmiyor olması sebepleriyle siber güvenlik anlamında neler yapıldığı şeffaf bir şekilde bilinmemektedir. Özellikle siber güvenliğin emniyet, askeri ve güvenlik güçlerinin tek elinde olması çıkarılmalıdır. Siber güvenliğin tam anlamıyla sağlanması için; siber saldırılara karşı etkin tedbir alınması, kurumların sosyal medyada yaratılan algı operasyonlarına karşı duyarlı olması, siber güvenlik farkındalığının geliştirilmesi, siber güvenliği sağlamada birimler arası koordinasyon ve işbirliğinin arttırılmaya çalışılması, siber altyapıların gelişimi için hem teknik hem de siyasi kararlılığın olması gerekmektedir.

Uluslararası arenada siber güvenlik yatırımları ve çalışmaları hız kazanmışken Türkiye'nin duyarsız kalması beklenemez. Terör örgütleri, çıkar grupları ve sınır aşan suç işleyen örgütler siber saldırıları her an kullanabilmektedirler. Bu açıdan Türkiye yurt içi veya yurt dışı kaynaklı siber saldırılara karşı her daim hazır olmak zorundadır. Ayrıca Türkiye sadece kendi resmi kurumlarını değil ekonomik

çıkarları gereği ticari şirket ve özel sektör girişimcilerini de korumak zorundadır. Türkiye'nin güvenlik politikalarında siber güvenliğin yeri ve önemi arttırılmalıdır. Daha etkili politikaların, farkındalık projelerinin ve somut adımların ihtiyaç olduğu açıktır.

Tüm bu sebeplerle Türkiye siber uzay kapasitesini geliştirmek zorundadır. Türkiye; siber güvenlik stratejisi, siber güvenlik eylem planları, siber güvenlik durum raporları ve eksiklilerini belirleyerek gereksinim duyulacak her türlü önlemelerin alınması zorunluluktur. Türkiye hem siber akademik düzey hem de pratik uygulamalar açısından ABD, Rusya, Japonya, Kore ve Çin ile karşılaştırıldığında zayıf olduğu görülecektir. Bu sebeple kendisini önce bu ülkelere karşı geliştirmesi ve bu ülkelerden gelebilecek siber tehditlere karşı korumaya almalıdır.

6. SONUÇ

Bu çalışmadaki hipotez, Türkiye'de siber güvenliğin ve siber farkındalığın yeterli olmaması ayrıca siber güvenliğe gereken önemin verilmediğini sonucunu varsaymaktadır. Bu çalışmanın yapılmasındaki amaçsa, siber güvenliğe verilen değerin ve önemin artması için bir farkındalık yaratmaktır. Çünkü siber güvenliğe verilen değeri yetersiz görüp ilgili kişilere, kurum ve kuruluşlara uyarı mahiyetinde bilgiler sunulmuştur.

Teknolojinin gelişmesiyle yeni tehdit algıları ortaya çıkmış olup bu tehdit algılarının siber güvenlik anlamında Türkiye'nin güvenlik konsepti veya güvenlik politikalarında sonuç doğurarak etkileyip etkilemediği araştırılmıştır. Bu etkinin yeterli düzeyde olmadığı vurgulanmış ve daha etkili politikaların, farkındalık projelerinin ve somut adımların ihtiyaç olduğu sonucuna varılarak uyarılarda bulunulmuştur.

Siber alanın özellikle küreselleşme ile birlikte ve teknolojinin her alana yayılıp bunun psikolojiden sosyolojiye, ticaretten ekonomiye kadar birçok alanda belirleyici bir unsur haline gelmesiyle sosyal bilimcilerde bu alanda çalışmalara başlamışlardır. Siber güvenliğin ve siber alanın son yıllarda gelişmesine rağmen hala işin başında olduğu da gerçekliktir. Siber uzay interaktif bir alan olup kullanıcılar ondan yararlanmakla birlikte ona katkı da sağlamaktadır. Bu sebeple siber uzay ile ilgili kavramlar ve literatür sürekli değişmekte ve gelişmektedir. Yeni ifadeler ve kullanılan emojiler ile diller, kültürler ve sosyal olarak insanlığı etkilemeye devam edecektir.

Büyük devrimler veya önemli olaylar insan haklarını geliştirmiştir. İnsan Hakları Sözleşmeleri insanın kazandığı tarihsel kazanımları ifade etmektedir. Bu sözleşmeleri benimseyip uygulamak insan olmanın gereği olup insanlık tarihi adına değerlidir. İnsan hakları sadece fiziksel olarak insan hakkı ihlal edilmemekte, internet ve sanal ortamda da insan hakları ihlal edilebilmektedir. Bu sebeple insan hakkı ihlallerinin önlenmesi için gerekli düzenlemeler interneti de kapsayacak şekilde yapılması gereklidir.

Türkiye'nin siber güvenlik politikalarının güvenlikleştirme boyutu yeterli düzeyde değildir. Güvenlik teorilerinin genel olarak tarihine bakıldığında devlet merkezli güvenlik anlayışından bireyi önceleyen güvenlik anlayışına doğru bir yol izlemiştir. Dolayısıyla bireylerin güvenliği önem arz etmektedir. Devletin vatandaşın güvenliğini öncelemesi özellikle Anadolu da tarihsel olarak gelen "insanı yaşat ki devlet yaşasın" düşüncesinden ileri gelmektedir.

Türkiye'de yasa koyucular kapsamlı olarak siber suçların yaptırımlarını arttırmak için çalışmalar yapmalı ve suçlarla etkin mücadele yöntemi geliştirilmelidir. Özellikle siber suçlara karşı yeni yöntemler geliştirilmeli ve teknik altyapıların güçlendirilmesi gerekmektedir. Tespit araçları ve mekanizmaları çoğaltılmalı, güvenlik ve hizmet sektörleri başta olmak üzere tüm sektörlerde siber güvenliğe verilen önem arttırılmalıdır.

Günümüzde siber güvenlik yatırımları ve çalışmaları hız kazanmıştır ve Türkiye'nin duyarsız kalmaması ve teknolojik yatırımlara hız vermesi gerekmektedir. Terör örgütleri, çıkar grupları ve sınır aşan suç işleyen örgütler siber saldırıları her an kullanabilmektedirler. Bu açıdan Türkiye yurt içi veya yurt dışı kaynaklı siber saldırılara karşı her daim hazır olmak zorundadır. Ayrıca Türkiye sadece kendi resmi kurumlarını değil ekonomik çıkarları gereği ticari şirket ve özel sektör girişimcilerini de korumak zorundadır.

Tüm bu sebeplerle Türkiye siber uzay kapasitesini geliştirmek zorundadır. Türkiye; siber güvenlik stratejisi, siber güvenlik eylem planları, siber güvenlik durum raporları ve eksiklileri belirleyerek gereksinim duyulacak her türlü önlemlerin alınması bir ihtiyaç değil zorunluluk olduğu ortaya çıkmıştır.

Son olarak, Türkiye'de siber güvenlik politikaları oluşturulurken güvenlik meselesi olarak algılanmasında yeterli olmadığı, vatandaşların siber tehdit algısının oluşmadığı, Türkiye'nin bu yeni tehdit algısına karşı güvenlik politikalarının yeterli seviyede ve önemde olmadığı düşünülmektedir. Bu sebeple siber güvenlik anlamında yeni bir tehdit algılaması olarak Türkiye'nin güvenlik politikaları içerisinde etkileri arttırılmalıdır. En azından politikalar oluşturulurken siber tehditlere karşı tedbir konusu ve farkındalık (bilinçlendirme) konuları daha sık gündeme gelmeli ve ele alınmalıdır.

KAYNAKÇA

Acar, H. & Pekcandanoğlu, M.(2020). Analysis of Cyber Security and Cyber Espionage Policies, Türkiye Rusya Araştırmaları Dergisi 3(Yaz 2020).Et: 18.09.2020 (https://www.dergipark.org.tr/tr/pub/trad/issue/55699/745123).

Akyeşilmen, N. (2018). Disiplinler arası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, Orion Kitabevi, Ankara.

Arı, T. (2011). Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği, MKM Yayıncılık, Bursa.

Arıboğan, Ü.& Ayman, G.& Dedeoğlu, B. (2005). Uluslararası İlişkiler Sözlüğü, der. Faruk Sönmezoğlu, Der Yayınları, İstanbul.

Baysal, B. & Lüleci, Ç. (2015). Kopenhag Okulu ve Güvenlikleştirme Teorisi, Güvenlik Stratejileri Dergisi, 11 (22) , 61-96. Et: 22.05.2020 (https://www.academia.edu/17191181/Kopenhag_Okulu_ve_G%C3%BCvenlikle%C5%9Ftirme_Teorisi).

BBC News Türkçe.9 Nisan 2015. Fransız yayın kuruluşu TV5 Monde'a siber 'IŞİD saldırısı'. E.t: 16.11.2020 (www.bbc.com/turkce/haberler/2015/04/150409_fransa_siber_saldiri).

Bendiek, A. (2012). European Cyber Security Policy, Stiftung Wissenschaft und Politik German Institute for International anf Security Affairs, Berlin.

Benedek, W.& Kettemann, M. (2013). İfade Özgürlüğü ve İnternet, Avrupa Konseyi, Türk Yargısının İfade Özgürlüğü Konusunda Kapasitesinin Güçlendirilmesi AB-AK Ortak Projesi, Baskı: Matbam Ajans, (https://rm.coe.int/16807005e4 e.t:12.02.2020).

Bıçakcı, S. (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler Akademik Dergisi, Cilt 10, Sayı 40 s. 101-130. Et: 07.05.2020 (https://www.uidergisi.com.tr/wp-content/uploads/2015/04/Bicakci-NATOnun-Gelisen-Tehdit-Algisi.pdf).

Bilgi Teknolojileri ve İletişim Kurumu. (2017). USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. E.t:18.03.2020 (https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi).

Bilgi Teknolojileri ve İletişim Kurumu. (2018). İnternet Bilgi İhbar Merkezi. E.t:18.03.2020 (https://www.ihbarweb.org.tr/).

Brent, L. (2019), NATO'nun siber uzaydaki rolü, Nato Dergisi, Et:29.20.2021 (https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydaki-rolue/index.html).

Cavelty, M.D. (2015). Cyber-Security, Comtemporary Security Studies, Thomson Digital, Zürih Et: 22.09.2020 (https://www.researchgate.net/publication/281631032).

Cihangir, M. (2020). Sosyal Medya Devriminin Neo-Politik Boyutları: Panoramik Bir İnceleme, Akademik Araştırmalar ve Çalışmalar Dergisi 12 (22): 186-196.

Çakmak, H. & Altunok, T. (2009). Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara.

Darıcılı,A.B. (2018). "Askerileştirilen ve Silahlandırılan Siber Uzay", (Ed. Ali ACARAVCI), Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri, ss.311-338, Nobel Yayınları, Ankara.

Eren, M. (2017). Avrupa Birliği'nin Siber Güvenlik Politikası, (1. Baskı). Beta Basım Yayım Dağıtım, İstanbul.

FIRAT, M. (2015). Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu. Hacettepe Hukuk Fakültesi Dergisi, 5 (2), 101-116. Retrieved from (https://dergipark.org.tr/tr/pub/hacettepehdf/issue/44831/557617).

Goyushov, S. (2019). Uluslararası İlişkilerde Güvenlik Çalışmalarına İlişkin Teorik Tartışmalar, Akademik Sosyal Araştırmalar Dergisi, Yıl: 7, Sayı: 88. Et: 22.05.2020 (http://www.asosjournal.com/DergiTamDetay.aspx?ID=14702).

Griffiths, M.&, Roach, S. C. &Solomon, M. S. (2011). Uluslararası İlişkilerde Temel Düşünürler ve Teoriler. Çev. CESRAN, Nobel Akademik Yayıncılık, Ankara.

Darıcılı, A.B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi, TESAM Akademi Dergisi, 6 (2), 11-33. Et: 20.05.2020 (https://dergipark.org.tr/tr/pub/tesamakademi/issue/48432/613517).

Kapani, M. (2008). Politika Bilimine Giriş, Bilgi Yayınevi, Ankara.

Karabulut, B. (2015). Güvenlik-"Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek", Barış Kitabevi, Ankara.

Kuzu, A. (Eylül 2019). MIT-MOSSAD-CIA-GLADIO Dünyanın En Büyük İstihbarat Servisleri, Kariyer Yayıncılık, İstanbul.

Kuzu, A. (Ağustos 2019). Dünyanın En Acımasız Örgütü MOSSAD, Kariyer Yayıncılık, İstanbul.

TASAM(Türk Asya Stratejik Araştırmalar Merkezi). (2004). Siber Terörizm Raporu, Et:05.05.2020 (https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf).

Türkiye Cumhuriyeti İç İşleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. Et:24.04.2020 (https://www.egm.gov.tr/siber/sibersucnedir).

Türkiye Cumhuriyeti İç İşleri Bakanlığı Kamu Düzeni ve Güvenliği Müsteşarlığı. (2017). Güvenlik Terimleri Sözlüğü. Kamu Düzeni ve Güvenliği Müsteşarlığı Yayınları, Ankara.

Ulusal Siber Olaylara Müdahale Merkezi (USOM) Siber Güvenliğe İlişkin Temel Bilgiler. (2014). Et:05.05.2020 (https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf).

Ünal, A.Y. (2020).Türkiye'nin siber saldırıları önleme merkezi kapılarını AA'ya açtı, Anadolu Ajansı: 08.02.2020. E.t:19.03.2020 (https://www.aa.com.tr/tr/turkiye/turkiyenin-siber-saldirilari-onleme-merkezi-kapilarini-aaya-acti/1727981).

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 58(1): 181-213.

Zedner, L. (2015). Güvenlik, çev. Defne Orhun, Optimist Yayın Grubu, İstanbul.